# Algebra di Insiemi

*Un'**algebra** di insiemi è un insieme che soddisfa le seguenti proprietà:*

*Costituisce un gruppo abeliano rispetto ad una operazione detta "unione"*

*Costituisce un gruppo abeliano rispetto ad una operazione detta "intersezione"*

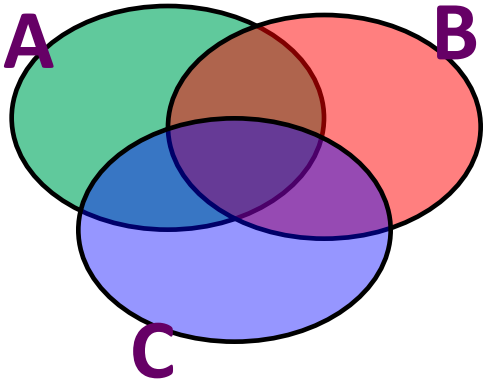
*Valgono entrambe le proprietà distributive:*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

# Algebra di Insiemi

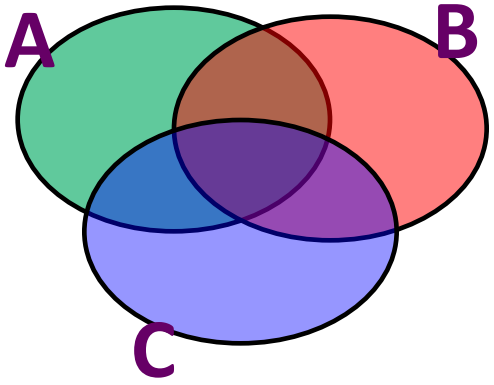
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

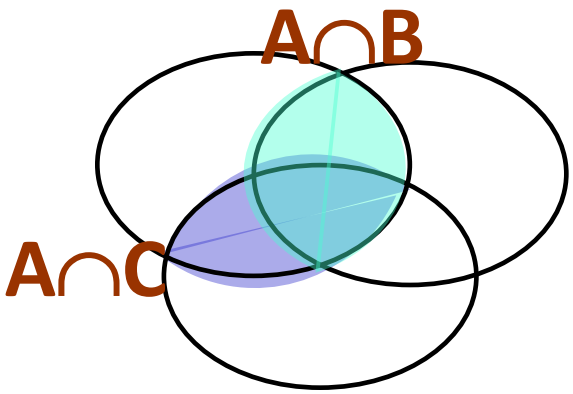


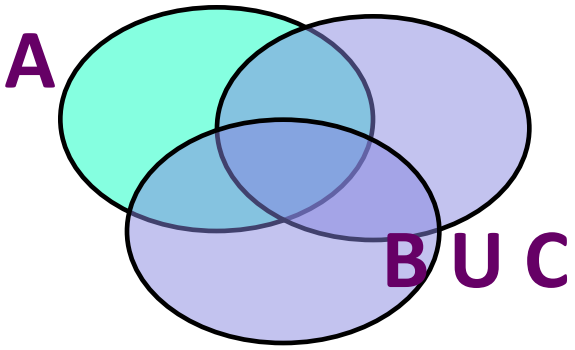

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

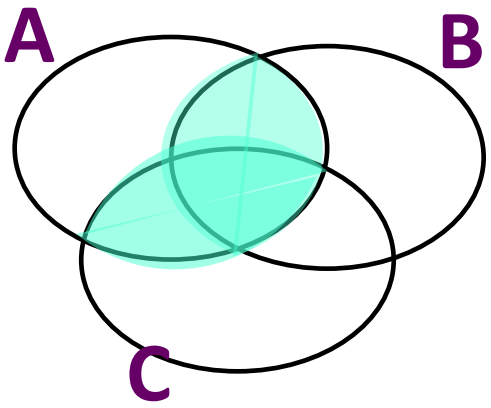
# Algebra di Insiemi

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$



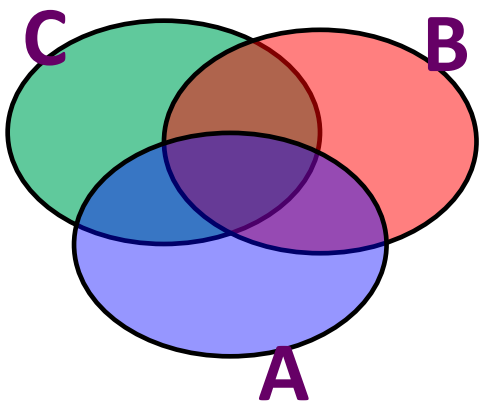



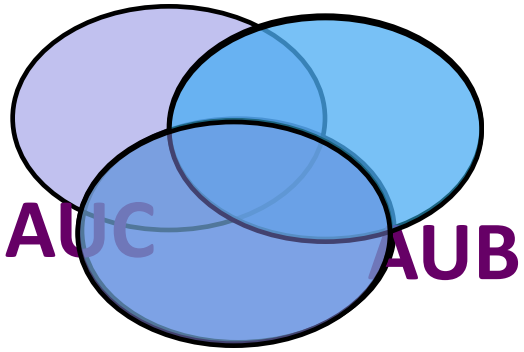



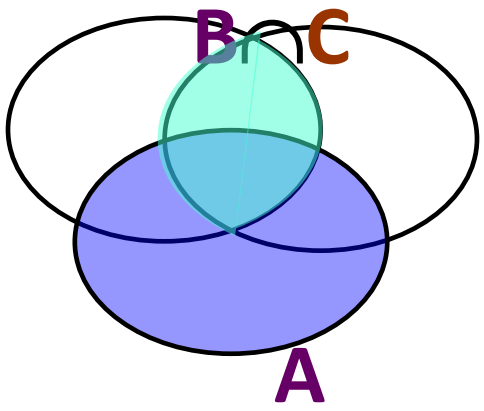



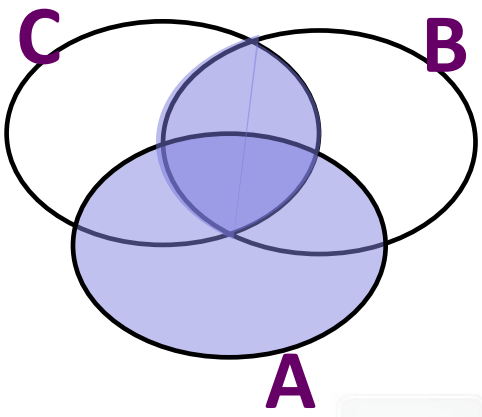
# Algebra di Insiemi

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$



# Cardinalità

*Due insiemi hanno la stessa cardinalità se esiste una corrispondenza biunivoca tra i loro elementi.*

*La condivisione di **cardinalità** è una relazione di **equivalenza**:*

*A <-> A* *(riflessiva)*

*A<-> B => B<->A* *(simmetrica)*

*f: A <-> B g: B <-> C -> g f : A <-> C* *(transitiva)*

*Dim: f(a)=b g(b)=c -> g(f(a))=c f, g, g(f()) Invertibili*

*"La cardinalità è una misura della complessità della rappresentazione"*

# Insiemi finiti

*Un insieme possiede **cardinalità n** se i suoi elementi sono in corrispondenza biunivoca con i numeri da*

*1 ad n. Cioè l'insieme possiede n elementi.*

*Un insieme in corrispondenza biunivoca con tutto N si dice **numerabile**.*

*In un insieme numerabile ad ogni elemento è possibile associare un numero naturale.*

*Un insieme possiede infiniti elementi se è possibile metterlo in corrispondenza biunivoca con un suo sottoinsieme proprio:*
*es: Naturali con i pari a<->2a*

# Albergo di Cantor

- *Nell'albergo di **Cantor** si danno convegno i matematici.*
- *All'ingresso ripongono i cappelli nell'apposita cappelliera.*
- *All'uscita ognuno prende un cappello ma ne avanzano 3*
- *Il giorno dopo invece all'uscita gli ultimi cinque rimangono senza cappello.*
- *Il terzo ed ultimo giorno i gestore li fa uscire in un ordine predefinito; tutti prendono il cappello e non ne avanza nessuno.*
- *Come si spiega il fenomeno?*
- *Come ha fatto il gestore? (Guidato da Cantor)*

*Georg Cantor*
*1845-1918*

# MCD mcm

- *MCD= Massimo Comune Divisore*
- *mod(a,d)=0  mod(b,d)=0;  d è divisore comune di a e b*
- *mod(a,M)=0  mod(b,M)=0  massimo dei divisori*
  *M=max(d)*

- *mcm= minimo comune multiplo*
- *mod(m',a)=0 mod(m',b)=0; m' è multiplo comune*
- *m=min(m')*
- *mcm= minimo dei multipli in comune*

# Notazioni

- *Notazione a|b "a divide b" mod(b,a)=0 b=a c*
- *(a,b) = MCD tra a e b = a || b*
- *Legame tra M=MCD(a,b) e m=mcm(a,b)*

***mcm(a,b)=a b /MCD(a,b)***

***m = a b /M  M = a b /m***

# Numeri Coprimi

- *I numeri a e b sono coprimi o primi tra loro se il loro Massimo Comune Divisore è l'unità.*

$$(a,b) = 1;\ \ a \,||\, b = 1 \ \ <\!\!-\!\!> MCD(a,b) = 1$$

- *Ovvero il minimo comune multiplo è il loro prodotto*

$$mcm(a,b) = a\ b / M = a\ b$$

# Algoritmo di Euclide

Εὐκλείδης (367-283 ac)

*Calcolo di a||b =MCD(a,b)*

*Passi:*

- *Si calcola il resto r della divisione di a per b*
- *Si ottiene una nuova coppia $a_1,b_1$*

*ponendo $a_1=b$, $b_1=r$.*

- *Si itera il procedimento fino a resto zero*

*a,b -> b,mod(a,b) -> ...-> $(a_n,b_n)$: $r_n=0$ ->*

***$b_n=a||b$***

# Algoritmo di Euclide

Εὐκλείδης (367-283 ac)

*Perché è corretto?*

*Perché se a e b sono divisibili per M*

*Allora anche a – bq=r è divisibile per M*

*Quindi (a,b)=(b,r)*

*Esempi:*

*(21,12)->(12,9)->(9,3) 9=3*3+0 -> (21,12)=3*

*(3 passi)*

*(15,20)->(15,5) 15=5*3+0 -> (15,20)=5*

*(3 passi)*

# Complessità algoritmo

- *Il resto è minore del più piccolo tra a e b e di a-b quindi è minore di a/2*
- *Ogni due passi entrambi i numeri sono minori della metà del maggiore due passi prima.*

- *Se a>b  next2log (a) in al più n= next2log (a) passi l'algoritmo termina.*
- *Quindi è complessità* ***al più*** *logaritmica.*

*Dim: mod(a,b) < min(b, a-b)< a/2*

*Vedremo una stima migliore in seguito*

# Esercizio Tabelle Pitagoriche in $Z_n$

*Ognuno ha fatto una tabellina di $Z_6$, $Z_7$ , $Z_{13}$ $Z_{17}$, $Z_{19}$ $Z_{35}$ …$Z_n$*

*Abbiamo osservato empiricamente che*

*-se n è primo su tutte le righe ci sono i numeri permutati.*

*-Se n non è primo nella tabellina appaiono degli zeri*

*-La tabella è simmetrica rispetto alle due diagonali principali*

# Inversi in $Z_n$

*"In $Z_n$ tutti i numeri coprimi con n ammettono un unico inverso": Hp (a,n)=1 (MCD=1)*

*Consideriamo b e c in $Z_n$ (n>b >c)*

*(a b = a c) mod n è impossibile:*

*a b – a c= a(b-c) = kn in Z*

*Per l'unicità della fattorizzazione k è multiplo di a e b-c è multiplo di n. Ma b < n c < n quindi b-c < n è impossibile.*

*Allora i numeri 1,2, … n-1 moltiplicati per a vengono mandati in loro stessi (ma permutati) e quindi uno di loro varrà 1 cioè è* ***l'inverso di a****.* ***(La riga a-esima della tabellina del prodotto contiene i numeri 1,2,…,n-1 permutati tra loro )***

# Inversi in $Z_n$

*"In $Z_n$ l'inverso di un numero coprimo con n è unico": Hp (a,n)=1 (MCD=1)*

*Consideriamo due inversi b e c in $Z_n$ (n>b >c)*

$$a\,b = 1 \pmod n$$

$$a\,c = 1 \pmod n$$

$$a\,(b-c) = 0 \pmod n$$

*Cioè* $a(b-c)=kn$

*impossibile perché a non è divisore di n e quindi* $b-c<n$ *dovrebbe essere un multiplo di n. Resta il caso* $b-c=0$.

*Cioè gli inversi coincidono.*

# Inversi in $Z_n$

*In $Z_n$ tutti i **divisori d dello zero** d|n non ammettono inverso. Hp n=d m.*

*Vediamo*

*d inv(d) = n k + 1= d (m k) +1  impossibile calcolando il resto rispetto a d*

*0 = 1 impossibile.*

*Cioè: d inv(d) – d m k= 1 -> d (inv(d)-d m)=1 (impossibile).*

*Se d|n : d a può essere uguale a d b*

*d (a-b)=0 se a-b multiplo di  n/d. **(La riga d-esima della tabellina del prodotto contiene degli zeri e non contiene 1)***

# Radici quadrate dell'unità in Zn

$a^2 = 1 \pmod n$

$(a+1)(a-1)=0 \pmod n$ cioè in N $(a+1)(a-1)=kn$

Esempio: $n=35 = 5x7$

$36=6^2= 5 \times 7 +1$ lo stesso per $35-6=29$

$a^2= 1 \pmod n$ ammette 4 soluzioni (1,6,29,34)

Cioè (1,6,-6,-1); $-6=35-6=29$; $-1=35-1=34$ (in $Z_{35}$)

# Teorema cinese dei resti

*Problema risolvere l'equazione diofantea*

$a\,x = b \pmod n$

*cioè* $ax = b + kn$ *(a,b,x,k in Z)*


**Διόφαντος III Sec**

*Quando l'equazione ha soluzioni?*

*1)(a,n)=1 "a ed n sono coprimi" esiste soluzione unica*

*2)(a,n)=d>1 "a non è primo con n"*

- *Se (a,n)=d e d|b ci sono d soluzioni distinte*
- *Se (a,n)=d, ma (d,b) < d nessuna soluzione*

# Teorema cinese dei resti

$a\,x = b \pmod n$ cioè $ax = b + kn$ $(k \text{ in } Z)$

**Caso 1)** $(a,n)=1$

*"Se a ed n sono coprimi esiste soluzione unica"*

*Moltiplichiamo ambo i membri per (inv(a))*

$a\,x = b + kn \rightarrow x = inv(a)\,b + k\,inv(a)\,n$

*Cioè* $x = inv(a)\,b \pmod n$.

*Unicità:*

$a\,x_1 = b \pmod n$, $a\,x_2 = b \pmod n$ $(supp\ x_1 > x_2)$

$a\,(x_1-x_2)=0 \pmod n \Leftrightarrow a\,(x_1-x_2) = kn$ $(in\ Z\ imposs.)$

# Teorema cinese dei resti

$a\,x = b \pmod n$ cioè $ax = b + kn$ $(k \text{ in } Z)$

**Caso 2)** $(a,n)=d$ "non è primo con n"

- Se $(a,n)=d$ ma $(d,b) < d$ nessuna soluzione

$ax = b + kn \rightarrow d\,(a/d)\,x = b + k\,d\,(n/d)$ impossibile.

- Se $(a,n)=d$ e $d|b$ ci sono $a'x=b' \pmod{n/d}$ ha soluzione $x'<n/d$ [ponendo $a'=a/d$; $b'=b/d$]

$d$ soluzioni distinte $x= x' + j\,(n/d)<n$ $(j=0,1,\ldots, d-1)$:

$a\,(x' + j(n/d)) = d\,a'\,x' + a\,j\,n/d = d\,b' + a'\,j\,n =$

$= b+(a'j)n$ cioè $b$ modulo $n$.

Unicità: $a\,(x_1-x_2)= 0 \Leftrightarrow a'\,(x_1-x_2) = n/d\,k$

# Sistema diofanteo

*Siano le due equazioni risolubili*

$a_1 x = b_1 \pmod{n_1}$ -> $x = x_1$ (Eq. 1)

$a_2 x = b_2 \pmod{n_2}$ -> $x = x_2$ (Eq. 2)

*Hp* $(n_1, n_2)=1$ *primi tra loro.*

*Th Esiste soluzione unica in* $n=n_1 n_2$.

$x = x_1 + k n_1 \pmod{n_1 n_2}$ (dalla Eq 1)

$x = x_1 + k n_1 = x_2 \pmod{n_2}$ (sost in Eq 2)

$k n_1 = x_2 - x_1 \pmod{n_2}$ *che ammette soluzione unica.*

*Quindi* $x = x_1 + k n_1 < n_1 n_2$ *soddisfa entrambe (in* $Z_n$*)*

# Sistema diofanteo

*Th inverso:*

*Se* $a\,x = b \pmod{n=n_1 n_2}$ *allora sodisfa il sistema.*

*Questo è ovvio perché*

$$a\,x = b + k n_1 n_2 \rightarrow \; mod(a,n_1)\,x = mod(b,n_1)$$

$$mod(a,n_2)\,x = mod(b,n_2) \text{ cioè}$$

$$a_1\,x = b_1 \pmod{n_1}$$

$$a_2\,x = b_2 \pmod{n_2}$$

*ponendo* $a_i = mod(a,n_i)$ $b_i = mod(b,n_i)$

*Abbiamo proiettato le equazioni in* $Zn_1$ *e* $Zn_2$.

# Teorema cinese dei resti

*Dato un sistema di k equazioni a due a due compatibili (cioè i cui moduli sono a primi tra loro)*

*Esiste sempre una soluzione in* $Z_{prodotto}$.

*Dim: Per induzione sul numero di equazioni k:*

*Il caso* $k=2$ *è già dimostrato.*

*Basta iterare la soluzione trovata nel caso di due equazioni ponendo* $n=n_1 n_2 n_3 \ldots n_{k-1} n_k = n_1 m_2$ .

$m_2 = n_2 n_3 \ldots n_{k-1} n_k$. *La soluzione in m esiste ed* $n_1$ *ed m sono coprimi tra loro, quindi esiste anche in n.*

# Sistema diofanteo

*Cosa succede se due $n_i$ non sono primi tra loro?*

- *Possiamo decomporre le equazioni corrispondenti in sistemi: $n_1/M$, $n_2/M$, ed $M=(n_1,n_2)$*
- *Due equazioni avranno lo stesso modulo M.*

- *Se sono compatibili si sostituisce la loro (o le loro) soluzione(i) e si ottiene un sistema risolubile.*

- *Se le due equazioni con lo stesso modulo (M) sono incompatibili, non esistono soluzioni per il sistema.*

# Molteplicità Sistema diofanteo

*Quante sono le soluzioni?*

*Se l'equazione k-esima ha $d_k$ soluzioni allora le soluzioni del sistema sono in totale:*

$$\#sol = d_1 d_2 d_3 \ldots d_{n-1} d_n$$

# Sistema diofanteo

*Esercizi*

*In* $Z_n$ $n=11 \times 13=143$ $Z_{143}$

*Risolvere il sistema*

$x= 3 \pmod{11}$

$x=5 \pmod{13}$

# Sistema diofanteo

*Esercizi*

*In* $Z_n$ $n=10 \times 13=130$ $Z_{130}$

*Risolvere il sistema*

$2x= 6 \pmod{10}$

$3x=5 \pmod{13}$

# Messaggio

*Il teorema dell'inverso ed il teorema cinese dei resti consentono di risolvere (dire se esistono ed esibire le soluzioni) tutti i sistemi di equazioni diofantee.*

*$Z_n$ è sempre un anello commutativo con unità.*

*Quando n è primo $Z_n$ è un campo, altrimenti no.*

*Quando n non è primo esistono i divisori dello zero ed il prodotto di due numeri non nulli può annullarsi. Le equazioni di secondo grado (eg: $x^2=1$) possono avere più di due soluzioni.*